Аладдин

Крипто БД
9 способов предотвращения утечки информации из СУБД

Содержание:

Резюме

В этом документе мы расскажем о способах решения распространенных проблем утечки информации из корпоративной базы данных с помощью Крипто БД.

Представленная здесь информация будет полезна специалистам:

- занимающимся информационной безопасностью;
- организующим защиту корпоративной базы данных;
- инженерам по эксплуатации информационных систем;
- администраторам баз данных;
- экспертам, реализующим стратегию импортозамещения в своей компании;

и организациям:

- чьи корпоративные базы данных построены на Oracle, MS SQL Server, PostgreSQL, Postgres Pro, Tibero, Jatoba;
- чьи базы данных нуждаются в надежной защите от внешних и внутренних нарушителей;
- находящимся в поисках замены тех механизмов защиты баз данных, которые были встроены в зарубежные решения, ушедшие с российского рынка;
- которым необходимо использовать сертифицированные средства защиты информации, соответствующие требованиям ФСБ России;
- имеющим статус КИИ.

Предотвращение утечек из СУБД

Назначение

Крипто БД— это система предотвращения утечек информации из корпоративных баз данных. Крипто БД поддерживает наиболее распространенные СУБД - Oracle, Microsoft SQL Server, PostgreSQL, Postgres Pro, Tibero и Jatoba.

Данный программный комплекс обеспечивает:

- защиту главных информационных активов организации (ERP, CRM, ИБС, ИСПДн и др.)
  - от утечек и кражи,
  - от внесения несанкционированных изменений и искажения чувствительной информации,
  - от несанкционированного доступа к критически важным данным администраторами СУБД;
- обезличивание персональных данных;
- прозрачное селективное шифрование критически важных данных в СУБД с использованием российских алгоритмов;
- двухфакторную аутентификацию пользователей при доступе к данным в СУБД;
- централизованное управление ключами шифрования, исключающее возможные несанкционированные действия администраторов БД;
- аудит действий пользователей и администратора баз данных при попытках доступа к защищаемой информации;
- реализацию требований регуляторов
  - по обеспечению конфиденциальности и целостности информации в СУБД,
  - по защите персональных данных,
  - по безопасности данных платежных карт PCI DSS,
  - по защите информационных систем организаций со статусом КИИ,
  - по моделям разделения доступа – дискретной и мандатной.

Ключевые преимущества для заказчиков

Система Крипто БД зарекомендовала себя как надежное средство защиты данных и обладает следующими преимуществами:

- использование быстрого и простого в реализации способа криптографической защиты информации в СУБД;
- минимальные затраты времени и ресурсов на организацию централизованной системы шифрования информации в базах данных;
- простота в эксплуатации и отсутствие необходимости существенного изменения производственных процессов для использования Крипто БД;
- ориентация на российский рынок (поддержка алгоритмов шифрования ГОСТ);
- импортозамещение средств защиты, встроенных в зарубежные СУБД;
- гибкий подход к ценообразованию;
- формирование юридически значимой доказательной базы для проведения расследований инцидентов информационной безопасности;

- возможность комплексного использования и "бесшовной" интеграции с целым рядом решений безопасности компании Аладдин;
- соответствие требованиям российского законодательства в использовании средств криптографической защиты;
- воплощение мировых практик в сфере создания продуктов и решений для обеспечения безопасности компаний.

Функции и возможности Крипто БД

На текущий момент система Крипто БД обладает рядом важнейших целевых функций обеспечения безопасности:

- шифрование данных;
- шифрование таблиц/столбцов базы данных;
- двухфакторная аутентификация;
- необратимое удаление данных;
- использование сертифицированных криптопровайдеров (при необходимости);
- централизованный мониторинг и аудит;
- разграничение доступа на основе ролевой модели.

Далее в документе будут описаны наиболее распространенные сценарии использования Крипто БД.

Бизнес-кейсы

1. Защита информации в СУБД при взломах информационных систем

При всем разнообразии сценариев реализации атак на информационные системы (далее ИС) злоумышленник, в конечном счете, стремится получить следующие возможности:

- управление функциями/параметрами ИС и, в частности, СУБД;
- управление содержимым системных журналов;
- хищение и компрометация информации из СУБД.

Основным назначением системы Крипто БД является предотвращение вышеперечисленных возможностей для злоумышленника в части защиты информации в СУБД от хищения и компрометации. Это обеспечивается путем шифрования защищаемой информации устойчивыми к криптоанализу методами, математически исключающими компрометацию информации в разумные для злоумышленника сроки.

Таким образом:

Крипто БД реализует такой тип защиты информации в СУБД, при котором не важен сценарий и успешность атаки на ИС. Даже похищенные данные будут надежно защищены шифрованием.

2. Защита от администратора СУБД

Современные информационные системы обладают рядом свойств, которые оказывают существенное влияние на безопасность обрабатываемой информации:

- сложность ИС и высокая сложность модели данных в СУБД (компетенциями обладает только администратор СУБД и разработчики);
- загруженность и высокая бизнес-значимость СУБД в ИС (параметрами производительности управляет только администратор СУБД);
- кадровый дефицит квалифицированных специалистов по администрированию СУБД.

В силу перечисленных обстоятельств администратор СУБД становится важной, не контролируемой и привилегированной ролью в ИС. При этом администраторы СУБД, зачастую, являются слабым звеном в организации защиты СУБД. Так возникает высокая вероятность инцидентов с негативными последствиями:

- утечка катастрофически больших объемов критичной, важной или секретной информации;
- отсутствие признаков реализации инцидента утечки и, как следствие, невозможность проведения полноценного расследования.

Система Крипто БД обеспечивает защиту информации от возможных преступных действий администратора СУБД:

- администратор СУБД не имеет ключей шифрования;
- все попытки доступа администратора СУБД к защищаемой информации фиксируются;
- реализован фундаментальный принцип разделения полномочий и ответственности;
- при этом администратор СУБД может выполнять свои обязанности без ограничений.

Таким образом:

Крипто БД является тем средством, которое позволяет обеспечить надежную защиту от привилегированных пользователей без ограничения возможностей администрирования базы данных.

3. Разграничение доступа к защищаемой информации

Разграничение доступа к информации является одной из основных функций безопасности информационных систем. В силу различных причин эта функция может быть реализована не самым оптимальным способом. Например:

- разграничение обеспечивается на уровне сервера приложений;
- функции разграничения реализуются пользовательским web-интерфейсом;
- разграничение производится без средств усиленной аутентификации пользователей.

Как правило, такую меру защиты достаточно просто обойти, манипулируя запросами к серверу приложений или подделывая web-запросы. При этом на уровне СУБД данные остаются незащищенными, доступ к данным не контролируется.

Такой подход к разграничению доступа применяется в подавляющем большинстве ИС, что по сути является критичной уязвимостью. Взлом подобной ИС не потребует от злоумышленника особых усилий, высокой квалификации и временных затрат.

Система Крипто БД обеспечивает надежное разграничение доступа пользователей к защищаемой информации на основе следующих функций:

- гибкая ключевая схема, позволяющая быстро и удобно назначить доступ одному или нескольким пользователям к защищаемому ресурсу;
- расширенная ролевая модель, позволяющая выделить функции контроля за доступом выделенному сотруднику безопасности.

Таким образом:

Крипто БД позволяет организовать контролируемый доступ к защищаемым данным в ИС на основе удобной матрицы доступа, обеспечив при этом высокий уровень надежности разграничения ролей.

4. Защита информации при размещении СУБД в "облаке"

Перенос ИС в "облако" сопровождает ряд негативных факторов, которые могут привести к масштабным утечкам критичной информации из принадлежащей ей СУБД:

- возникает возможность физического доступа третьих лиц (например, сотрудники облачного оператора) к серверам ИС/СУБД;
- доступ третьих лиц к серверам ИС/СУБД никак не контролируется и не фиксируется на стороне заказчика услуги.

При размещении серверов ИС в "облаке" перспективы злоумышленника получить желаемое значительно расширяются за счет возможности физического и административного доступа к этим серверам.

Использование системы Крипто БД для защиты информации в СУБД при размещении серверов ИС в "облаке" существенно сокращает риск кражи и потери конфиденциальности информации. При успешном взломе ИС злоумышленник, в конечном счете, получит доступ к надежно зашифрованной информации без возможности ее использования в преступных целях.

Таким образом:

Использование системы Крипто БД в качестве защитной меры при переносе ИС в "облако" позволяет снизить риски, связанные с неконтролируемым доступом посторонних лиц к серверам СУБД.

5. Защита резервных копий и архивов информационных систем

Задача по защите информации в архивах резервных копий ИС является наиболее сложно осуществимой для заказчиков в силу ряда условий, диктуемых потребностями бизнеса:

- функции защиты архивов не должны нарушать сложившиеся процессы и методы резервирования информации;
- при краже/хищении архивов не должно возникать угроз, связанных с потерей конфиденциальности архивной информации;
- процесс восстановления информации из защищенных архивных копий должен быть прозрачным и совместимым с процедурами восстановления;
- при хранении защищенных архивов должно соблюдаться соответствие ряду нормативных требований РФ (например 187-ФЗ, Приказ 21 ФСТЭК России и т.п.)

При использовании системы Крипто БД информация в таблицах СУБД уже защищена шифрованием. Поэтому процедуру резервного копирования не надо изменять или перестраивать. Данные, попадающие в архивы резервных копий, будут по умолчанию защищены. Хищение такой информации не будет порождать возникновения новых угроз, связанных с потерей конфиденциальности хранимой информации.

Таким образом:

Важнейшим преимуществом системы Крипто БД является возможность решения задачи защиты архивных копий без дополнительных затрат в настройке, администрировании и сопровождении средств защиты информации.

6. Маскирование и деперсонализация информации

Многие организации различных сфер деятельности сталкиваются с необходимостью построения и ввода в эксплуатацию новых ИС, включая их разработку и тестирование. Ввод в эксплуатацию каждой новой ИС (корпоративного приложения, технического ИТ-средства и т.п.) всегда сопровождается процессом формирования тестовых сред и наполнения их тестовыми данными. Для этого компаниям приходится реплицировать базы данных для обеспечения процесса тестирования систем. Здесь перед бизнесом встает целый список противоречивых вопросов, как защитить информацию в реплицированных наборах данных, при условии, что:

- реплицируемые наборы данных должны быть актуальными;
- размер выборки данных в наборах должен соответствовать реальному объему информации;
- в реплицируемые набору неизбежно попадает критически важная и конфиденциальная информация.

Процесс согласования выдачи данных их владельцами и назначение ответственных лиц за процесс тестирования занимает неопределенное время, приходится ждать гораздо больше планируемого в рамках проекта времени. Все эти условия усугубляются необходимостью деперсонализации передаваемых данных. В связи с этим, задача по маскированию критически важной, конфиденциальной информации приобретает высокую значимость.

Одной из важнейших функций системы Крипто БД является маскирование. Система реализует наиболее продвинутый метод маскирования – "динамическое маскирование":

- каждому столбцу данных может быть определена собственная маска;
- маски могут настраиваться по формату и внешнему виду;
- маски могут генерироваться из диапазонов заданных значений;
- маскируется актуальная информация.

При формировании и перемещении реплицируемого набора данных используются маски, в то время как реальные конфиденциальные данные никогда не покидают СУБД.

Таким образом:

Использование системы Крипто БД позволяет обеспечить разработчиков пилотных зон реплицированными наборами данных, которые позволят обеспечить полноценное тестирование ИС в тестовых средах. При этом задача обеспечения маскирования информации не потребует отдельных усилий и будет решаться в общей канве выполнения задач по защите данных в СУБД.

7. Надежное уничтожение персональных данных

Вывод устаревшей ИС из эксплуатации - неминуемый этап жизненного цикла любой системы. В процессе вывода из эксплуатации данные, хранимые в СУБД этой ИС, должны быть надежно уничтожены. Термин "надежно" предполагает в данном случае отсутствие возможности восстановления уничтоженных данных. К надежному уничтожению данных прибегают не только в процессе вывода ИС из эксплуатации, но также в ходе модернизации системы, изменения информационной модели, оптимизации структур данных в СУБД и т.д.

Зачастую, для решения подобных задач используются узкоспециализированные программные инструменты. Их приобретение, установка и администрирование задействует существенные финансовые и временные ресурсы. При использовании данных средств безусловно возникает вопрос - насколько надежно уничтожаются данные? Ответить на такой вопрос достаточно сложно.

При использовании системы Крипто БД, защищающей всю важную критичную или конфиденциальную информацию, проблема организации процесса надежного уничтожения данных уже решена. Все защищаемые данные надежно зашифрованы стойкими алгоритмами шифрования (в соответствии с требованиями ГОСТ 28147-89, ГОСТ 34.12-2015). В случае неавторизованного восстановления уничтоженной информации злоумышленник получит зашифрованный массив данных, расшифрование которого для него будет невозможно в разумных пределах затрат ресурсов и времени.

Таким образом:

Система Крипто БД позволяет решать сопутствующие прикладные задачи по надежному уничтожению информации из СУБД, обеспечивая при этом существенную экономию усилий и финансовых средств сотрудников ИТ и ИБ подразделений.

8. Независимый аудит событий доступа к информации

Одной из ключевых задач ИБ-службы компании является мониторинги расследование инцидентов информационной безопасности. В рамках данных мероприятий ИБ-специалисты собирают внушительное количество информации о системных событиях, а также информацию о событиях безопасности. Адекватность и эффективность результатов расследования ИБ-инцидентов зависит, в большей степени, от актуальности и достоверности собираемых данных.

Используя защиту информации посредством системы Крипто БД компания получает возможность организации сбора и обработки информации о событиях доступа пользователей или администраторов к защищаемым данным, хранящимся в СУБД. Механизм журналирования событий системы Крипто БД имеет ряд преимуществ:

- фиксация событий доступа к защищаемой информации;
- передача зафиксированной информации внешней системе (например, SIEM);
- защита процедур логирования от возможных злонамеренных действий администратора СУБД.

Таким образом:

Система Крипто БД позволяет организовать независимый процесс фиксации и передачи информации о фактах доступа к защищаемой информации. При этом администратор СУБД не имеет возможности изменения или чтения защищаемой информации.

9. Complience или выполнение требований нормативных документов

Каждое мероприятие по защите информации так или иначе соотносится с определенным набором требований в области информационной безопасности. Задачи по приведению ИС в соответствие требованиям различных отечественных или зарубежных стандартов являются основой деятельности ИБ-службы. Мероприятия по предотвращению утечек конфиденциальной информации из СУБД не являются исключением.

Крипто БД позволяет успешно решить ряд задач при проведении следующих мероприятий:

- Выполнение требований 152-ФЗ (приказ №21 ФСТЭК России), в части защиты персональных данных:
  - разграничение доступа к ПДН в СУБД,
  - реализация двухфакторной аутентификации при доступе к ПДн в СУБД,
  - мониторинг и логирование событий доступа к защищаемым данным;
- Выполнение требований стандарта безопасности PCI DSS
  - шифрование и маскирование PAN в подсистемах процессинга,
  - маскирование данных платежных карт,
  - надёжная защита ключей шифрования на протяжении их жизненного цикла,
  - прозрачное встраивание в готовые информационные системы,
  - аудит и мониторинг доступа к защищённым данным,
  - централизованное управление функциями безопасности (ключи шифрования, аудит, пользователи и т.п.),
  - контроль целостности собственного ПО и служебной информации;
- Выполнение требований ФЗ-187 в части защиты данных систем критической инфраструктуры
  - обеспечение целостности служебной информации в СУБД,
  - обеспечение конфиденциальности данных, обрабатываемых в критических информационных инфраструктурах (КИИ);
- Выполнение требований Приказа №17 ФСТЭК в части защиты конфиденциальной информации обрабатываемой в ГИС
  - разграничение доступа к ПДН в СУБД,
  - реализация двухфакторной аутентификации при доступе к ПДн в СУБД,
  - мониторинг и логирование событий доступа к защищаемым данным.

Таким образом:

Система Крипто БД органично вписывается в состав эффективного инструментария ИБ-службы организации, позволяя совместить выполнение требований нормативных документов и предотвращение актуальных и критичных угроз информационной безопасности.

Возможности импортозамещения и соответствие требованиям регулирующих органов РФ

Система Крипто БД соответствует требованиям ФСБ России. Результаты прохождения сертификационных испытаний подтверждают, что средство криптографической защиты информации Крипто БД версии 3.0 (исполнения 1, 2) удовлетворяет "Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений составляющих государственную тайну" по классам КС1 (исполнение 1), КС2 (исполнение 2), а также "Специальным требованиям к средствам криптографической защиты, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р)" и "Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну" по уровню $КС_{Б}$.

В подтверждение этому выдано положительное заключение N° 149/3/2/1/1334 от 14.06.2023.

Ожидаемый срок получения сертификата соответствия – III квартал 2023 г.

Система Крипто БД является полностью отечественной разработкой, состоит в едином реестре отечественного ПО (реестровые записи №509, 518, 4292, 4293) и может применяться для импортозамещения зарубежных средств защиты.

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин — ведущий российский вендор-разработчик и производитель
ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры

https://t.me/aladdinrd https://vk.com/aladdinrd